

1 **Amendments to the Claims:**

2 This listing of claims will replace all prior versions, and listings, of claims in the application:

3  
4 1. (Currently Amended) A method of preventing piracy of a given software application  
5 comprising the steps of:

6 assigning a unique identification code to each authentic copy of such software application;

7 installing the software application in a data storage element on a user's computer;

8 configuring the software application to require service data to activate at least part of its  
9 functionality;

10 ~~requiring a user to enter into the user's computer identifying data that identifies the user;~~

11 requiring the user to communicate user data over a communications network to a remote  
12 service provider system, the user data being derived, at least in part, from ~~the identifying data that~~  
13 ~~identifies the user, and being derived, at least in part, from the unique identification code;~~

14 ~~archiving user data received from the user over the communications network in a data~~  
15 ~~storage element of the remote service system, said remote service system being connected to said~~  
16 ~~communications network and designated to receive said user data;~~

17 ~~comparing~~ examining received user data ~~for each to derive the~~ unique identification code  
18 associated with the copy of the software application installed by said user with previously archived  
19 user data corresponding to the same unique identification code to determine whether said user is  
20 pirating

21 counting the number of times an attempt has been made to obtain said service data in order  
22 to activate at least part of the functionality of said software application assigned to such unique  
23 identification code; and

24 selectively transmitting service data to the user's computer ~~from said remote service system~~  
25 when said remote service provider system determines that ~~said service data should be transmitted~~  
26 the number of times an attempt has been made to obtain said service data in order to activate at  
27 least part of the functionality of said software application assigned to such unique identification  
28 code is fewer than a predetermined threshold, said user's computer being connected to said

1 communications network and designated to storablely receive said service data.

2  
3 2. Canceled.

4  
5 3. (Previously presented) The method as in Claim 1,

6 wherein said user data comprises the unique identification code that identifies said software  
7 application installed on a data storage element of the user's computer.

8  
9 4. (Previously presented) The method as in Claim 1,

10 wherein said user data includes ~~said~~ identifying data that identifies the user.

11  
12 5. (Previously presented) The method as in Claim 1,

13 wherein said user data includes product information relating to said software application  
14 installed on the data storage element of the user's computer.

15  
16 6. Canceled.

17  
18 7. Canceled.

19  
20 8. Canceled.

21  
22 9. Canceled.

23  
24 10. Canceled.

25  
26 11. Canceled.

27  
28 12. (Currently amended) The method as in Claim 1,

1 wherein said service data is maintained in the data storage element of the remote service  
2 provider system.

3  
4 13. (Previously presented) The method as in Claim 12,

5 wherein said service data comprises at least one program code sequence that activates at  
6 least part of the functionality of said software application stored on said data storage element of the  
7 user's computer.

8  
9 14. (Previously presented) The method as in Claim 12,

10 wherein said service data includes at least one program code sequence that results in a  
11 promotional message that may be displayed to said user on the user's computer system.

12  
13 15. Canceled.

14  
15 16. Canceled.

16  
17 17. Canceled.

18  
19 18. (Currently amended) The method as in Claim 1,

20 wherein said service data is derived at least in part from said user data stored on said data  
21 storage element of said remote service provider system.

22  
23 19. (Currently amended) The method as in Claim 1,

24 wherein the step of selectively transmitting said service data is an uploading event in which  
25 said service data is automatically transferred from said remote service provider system and storable  
26 received by the user's computer system.

27  
28 20. (Currently amended) The method as in Claim 1,

1 wherein the step of selectively transmitting said service data is an uploading event in which  
2 said service data is manually transferred from said remote service provider system and storable  
3 received by the user's computer system.

4  
5 21. (Currently amended) The method as in Claim 1,

6 wherein the step of selectively transmitting said service data is a downloading event in  
7 which said service data is made available to said user from said remote service provider system,  
8 and wherein said user downloads said service data into the user's computer system.

9  
10 22. (Previously presented) The method as in Claim 1,

11 wherein said software application includes a program code sequence that identifies said  
12 software application stored on said data storage element of the user's computer system, said  
13 software application additionally being responsive to a second program code sequence that  
14 activates at least part of the functionality of said software application, and which is transmitted to  
15 the user's computer system via said communications network.

16  
17 23. (Currently Amended) A system for preventing piracy of a given software application, said  
18 software application having a unique identification code associated therewith, and said software  
19 application requiring service data to activate at least part of the functionality of said software  
20 application, said system comprising:

21 a user computer system on which a user desires to operate the software application, said  
22 user system being connected to a communications network to transmit user data and to ~~storable~~  
23 receive said service data, said user data being derived at least in part from ~~identifying data entered~~  
24 ~~by the user on the user computer system which identifies the user, and being derived at least in part~~  
25 ~~from~~ said unique identification code;

26 a remote service computer system connected to said communications network to ~~storable~~  
27 receive user data transmitted over the communications network from the user computer system said  
28 remote service computer system transmitting said service data to said user computer system ~~over~~

1 ~~said communications network~~ when it is determined that ~~said user is not pirating~~ the number of  
2 times an attempt has been made to obtain said service data in order to activate at least part of the  
3 functionality of said software application assigned to such unique identification code is fewer than  
4 a predetermined threshold.

5  
6  
7 24. (Previously presented) The system as in Claim 23

8 wherein said remote service computer system includes a data storage element for archiving  
9 user data for each unique identification code, wherein said remote service computer system  
10 compares user data received from the user computer system to user data previously archived by said  
11 remote service computer system relative to the same unique identification code, and wherein said  
12 remote service computer system transmits said service data to said user computer system when said  
13 user data received by said remote service computer system is consistent with user data previously  
14 archived by said remote service computer system relative to the same unique identification code.

15  
16 25. (Previously presented) The system as in Claim 23

17 wherein said service data is maintained by said remote service computer system in the data  
18 storage element used to archive said service data.

19  
20 26. (Previously presented) The system as in Claim 23

21 wherein said service data consists, at least in part, of an activation code sequence to activate  
22 at least part of the functionality of the software application.

23  
24 27. (Currently amended) The system as in Claim 23

25 wherein said service data is ~~automatically~~ transferred by said remote service computer  
26 system without human intervention and ~~storably~~ received by said user computer system.

27  
28 28. (Previously presented) The system as in Claim 23

1 wherein said remote service computer system manually transfers said service data from said  
2 remote service computer system to said user system.

3  
4 29. (Previously presented) The system as in Claim 23

5 wherein said remote service computer system makes said service data available to said user  
6 from said remote service system, said user being able to download said service data into said user  
7 computer system.

8  
9 30. (Previously presented) The system as in Claim 23,

10 wherein said software application includes a program code sequence that identifies said  
11 software application stored on said data storage element of said user system, said software  
12 application additionally being responsive to a second program code sequence that activates at least  
13 part of the functionality of said software application, and which is transmitted to said user system  
14 via a communications network.

15  
16 31. (Currently amended) A method of preventing piracy of a given software application  
17 comprising the steps of:

18 assigning a unique identification code to each authentic copy of such software application;  
19 installing the software application in a data storage element on a user's computer;  
20 configuring the software application to require service data to activate at least part of its  
21 functionality ;

22 ~~requiring a user to enter into the user's computer identifying data that identifies the user;~~  
23 requiring the user to communicate user data over a communications network to a remote  
24 service provider system, the user data being derived, at least in part, from ~~the identifying data that~~  
25 ~~identifies the user, and being derived, at least in part, from the unique identification code;~~

26 examining received user data ~~received by the remote service system from the user's~~  
27 ~~computer to determine whether the user is pirating~~ derive the unique identification code associated  
28 with said ~~the~~ software application;

1 determining the number of times an attempt has been made to obtain said service data in  
2 order to activate at least part of the functionality of said software application assigned to such  
3 unique identification code;

4 selectively transmitting service data to the user's computer ~~from said remote service system~~  
5 ~~when said remote service system determines that the user is not pirating the software application~~  
6 the number of times an attempt has been made to obtain said service data is fewer than a  
7 predetermined threshold; and

8 ~~stably~~ receiving the transmitted service data within ~~the data storage element of the user's~~  
9 computer, wherein said service data is used to activate at least part of the functionality of the  
10 software application.

11  
12 32. (Previously presented) The method recited by Claim 31 further including the step of  
13 archiving user data received from users over the communications network in a data storage  
14 element of the remote service system.

15  
16 33. (Previously presented) The method recited by Claim 32,  
17 wherein received user data for each unique identification code is compared with previously  
18 archived user data corresponding to the same unique identification code.

19  
20 34. (Previously presented) The system as recited in Claim 26,  
21 wherein said service data includes at least one program code sequence that results in a  
22 promotional message that may be displayed to said user on said user computer system.

23  
24 35. (Currently amended) A method of preventing piracy of a given software application  
25 comprising the steps of:

26 a. assigning a unique identification code to each authentic copy of such software  
27 application;

28 b. installing the software application in a data storage element on a user's computer;

1 c. configuring the software application to require service data ~~to activate~~ , said service data  
2 being a necessary component to enable at least part of ~~its~~ the software's functionality;

3 d. requiring the user to communicate user data to a remote service provided ~~system~~, the  
4 user data being derived, at least in part, from ~~identifying data that identifies the user, and being~~  
5 ~~derived, at least in part, from~~ the unique identification code;

6 e. examining received user data ~~received by the remote service system~~ to determine  
7 ~~whether the user is pirating~~ derive the unique identification code associated with said ~~the~~ software  
8 application;

9 f. determining the number of times an attempt has been made to obtain said service data in  
10 order to activate at least part of the functionality of said software application assigned to such  
11 unique identification code;

12 g. selectively transmitting service data to the user's computer ~~from said remote service~~  
13 ~~system~~ when ~~said remote service system determines that the user is not pirating~~ the number of  
14 times an attempt has been made to obtain said service data in order to activate the software  
15 application assigned to such unique identification code is fewer than a predetermined threshold;  
16 and

17 g. h. ~~storably~~ receiving the transmitted service data within ~~the data storage element of the~~  
18 user's computer, wherein said service data is used to activate at least part of the functionality of the  
19 software.

20  
21 36. (Previously presented) The method recited by Claim 35 further including the step of archiving  
22 user data received from users.

23  
24 37. (Previously presented) The method recited by Claim 36,  
25 wherein received user data for each unique identification code is compared with previously  
26 archived user data corresponding to the same unique identification code.

27  
28 38. (Currently amended) A method of preventing piracy of a given software application



1 comprising the steps of:

2 a. assigning a unique identification code to each authentic copy of such software  
3 application;

4 b. installing the software application in a data storage element on a user's computer;

5 c. configuring the software application to require service data, said service data being a  
6 necessary component to enable at least part of the software's functionality;

7 d. requiring the user to communicate user data to a ~~remote~~ service provider system, the user  
8 data being derived, at least in part, from ~~identifying data that identifies the user, and being derived,~~  
9 ~~at least in part, from~~ the unique identification code;

10 e. examining received user data ~~received by the remote service system to determine whether~~  
11 ~~the user is pirating~~ derive the unique identification code associated with said the software  
12 application;

13 f. ascertaining the number of times an attempt has been made to obtain said service data in  
14 order to activate at least part of the functionality of said software application assigned to such  
15 unique identification code ~~selectively transmitting service data to the user's computer from said~~  
16 ~~remote service system when said remote service system determines that the user is not pirating the~~  
17 ~~software application; and~~

18 g. determining whether the number of times an attempt has been made to obtain said service  
19 data is fewer than a predetermined threshold ~~stably receiving the transmitted service data within~~  
20 ~~the data storage element of the user's computer to activate at least part of the software's~~  
21 ~~functionality .~~

22  
23 39. (Previously presented) The method recited by Claim 38 further including the step of archiving  
24 user data received from users.

25  
26 40. (Previously presented) The method recited by Claim 39,

27 wherein received user data for each unique identification code is compared with previously  
28 archived user data corresponding to the same unique identification code.

1 41. (New) The method recited by Claim 31 wherein said received service data is stored within the  
2 data storage element of the user's computer.

3  
4 42. (New) The method recited by Claim 35, wherein said received service data is stored within the  
5 data storage element of the user's computer.

6  
7 43. (New) The method recited by Claim 38 further including the step of communicating service  
8 data to the user to activate at least part of the said software's functionality.

9  
10 44. (New) The method recited by Claim 43, wherein said communicated service data is stored  
11 within the data storage element of the user's computer.

12  
13 45. (New) A method of preventing piracy of a given software application comprising the steps of:  
14 assigning a unique identification code to each authentic copy of such software application;  
15 installing the software application in a data storage element on a user's computer;  
16 configuring the software application to require service data to activate at least part of its  
17 functionality;

18 requiring the user to communicate user data to a remote service provider, the user data being  
19 derived, at least in part, from the identifying data that identifies the user, and being derived, at least  
20 in part, from the unique identification code;

21 archiving identifying data received from a user for each unique identification code if no such  
22 identifying data has previously been archived for such unique identification code;

23 comparing received identifying data associated with a unique identification code with  
24 previously archived identifying data corresponding to the same unique identification code if such  
25 identifying data has previously been archived;

26 selectively transmitting service data to the user's computer when no such identifying data  
27 has previously been archived for such unique identification code;

28 selectively transmitting service data to the user's computer when the received identifying

1 data is consistent with previously archived data for the same unique identification code; and  
2 receiving the transmitted service data within the data storage element of the user's computer  
3 to activate at least part of the functionality of the software application.  
4

5 46. (New) The method recited by claim 45 wherein said step of selectively transmitting service  
6 data to the user's computer when the received identifying data is consistent with previously  
7 archived data for the same unique identification code includes the steps of:

- 8 a. determining the number of times that said service data has been requested; and
- 9 b. refusing transmission of said service data when the number of times that said service data  
10 has been requested exceeds a predetermined threshold.

11  
12 47. (New) The method recited by claim 45 including the steps of:

- 13 a. determining the number of times that received identifying data is not consistent with  
14 previously archived data for the same unique identification code; and
- 15 b. refusing transmission of said service data when the number of times that received  
16 identifying data is not consistent with previously archived data for the same unique identification  
17 code exceeds a predetermined threshold.

18  
19 48. (New) The method recited by Claim 45 further including the step of archiving identifying data  
20 received from a user for each unique identification code subsequent to an initial archiving of  
21 identifying data pertaining to the same unique identification code.  
22

23 49. (New) The method recited by Claim 45 wherein said received service data is stored within the  
24 data storage element of the user's computer.  
25

26 50. (New) A method of preventing piracy of a given software application comprising the steps of:  
27 assigning a unique identification code to each authentic copy of such software application;  
28 installing the software application in a data storage element on a user's computer;

1 configuring the software application to require service data to activate at least part of its  
2 functionality;  
3 requiring the user to communicate user data to a service provider, the user data being  
4 derived, at least in part, from the identifying data that identifies the user, and being derived, at least  
5 in part, from the unique identification code;  
6 archiving identifying data received from a user for each unique identification code if no such  
7 identifying data has previously been archived for such unique identification code;  
8 comparing received identifying data associated with a unique identification code with  
9 previously archived identifying data corresponding to the same unique identification code if such  
10 identifying data has previously been archived;  
11 determining if identifying data has previously been archived for such unique identification  
12 code, and if so, whether such previously archived data is consistent with newly-received identifying  
13 data for the same unique identification code.

14  
15 51. (New) The method recited by Claim 50 further including the step of communicating service  
16 data to the user to activate at least part of the said software's functionality.

17  
18 52. (New) The method recited by Claim 51, wherein said communicated service data is stored  
19 within the data storage element of the user's computer.

20  
21 53. (New) The method recited by claim 50 wherein said step of communicating service data to the  
22 user further includes the steps of:

- 23 a. determining the number of times that said service data has been requested; and  
24 b. refusing transmission of said service data when the number of times that said service data  
25 has been requested exceeds a predetermined threshold.

26  
27 54. (New) The method recited by Claim 50 further including the step of archiving identifying data  
28 received from a user for each unique identification code subsequent to an initial archiving of

1 identifying data pertaining to the same unique identification code.

2  
3 55. (New) A method of preventing piracy of a given software application comprising the steps of:  
4 assigning a unique identification code to each authentic copy of such software application;  
5 installing the software application in a data storage element on a user's computer;  
6 configuring the software application to require service data to activate at least part of its  
7 functionality;  
8 requiring the user to communicate user data to a service provider, the user data being  
9 derived, at least in part, from the identifying data that identifies the user, and being derived, at least  
10 in part, from the unique identification code;  
11 comparing received identifying data associated with a unique identification code with  
12 previously archived identifying data corresponding to the same unique identification code if such  
13 identifying data has previously been archived;  
14 selectively communicating service data to the user when the received identifying data is  
15 consistent with previously archived data for the same unique identification code; and  
16 receiving the communicated service data wherein said service data is used to activate at least  
17 part of the functionality of the software.

18  
19 56. (New) The method recited by claim 55 wherein said step of selectively communicating service  
20 data to the user when the received identifying data is consistent with previously archived data for  
21 the same unique identification code includes the steps of:

22 a. determining the number of times that said service data has been requested; and  
23 b. refusing communication of said service data when the number of times that said service  
24 data has been requested exceeds a predetermined threshold.

25  
26 57. (New) The method recited by claim 55 including the steps of:

27 a. determining the number of times that received identifying data is not consistent with  
28 previously archived data for the same unique identification code; and

1           b. refusing communication of said service data when the number of times that received  
2 identifying data is not consistent with previously archived data for the same unique identification  
3 code exceeds a predetermined threshold.

4  
5 58. (New) The method recited by Claim 55 further including the step of archiving identifying data  
6 received from a user for each unique identification code.

7  
8 59. (New) The method recited by Claim 55 wherein said received service data is stored within the  
9 data storage element of the user's computer.

10  
11 60. (New) The method as in Claim 1 further comprising the steps of:

12           requiring a user to provide identifying data that identifies the user;

13           deriving the user data that is communicated to the remote service provider, at least in part,  
14 from the identifying data that identifies the user;

15           archiving received identifying data in a data storage element of the remote service provider  
16 for each unique identification code; and

17           comparing the received identifying data for a given unique identification code with  
18 previously archived identifying data for the same unique identification code to determine whether  
19 they match each other.

20  
21 61. (New) The method as in Claim 60 including the step of restricting transmission of said service  
22 data to the user's computer if said received identifying data for a given unique identification code  
23 does not match previously archived identifying data for the same unique identification code.

24  
25 62. (New) The method as in Claim 31 further comprising the steps of:

26           requiring a user to provide identifying data that identifies the user;

27           deriving the user data that is communicated to the remote service provider, at least in part,  
28 from the identifying data that identifies the user;

1 archiving received identifying data in a data storage element of the remote service provider  
2 for each unique identification code; and  
3 comparing the received identifying data for a given unique identification code with  
4 previously archived identifying data for the same unique identification code to determine whether  
5 they match each other.

6  
7 63. (New) The method as in Claim 62 including the step of restricting transmission of said service  
8 data to the user's computer if said received identifying data for a given unique identification code  
9 does not match previously archived identifying data for the same unique identification code.

10  
11 64. (New) The method as in Claim 35 further comprising the steps of:

12 requiring a user to provide identifying data that identifies the user;  
13 deriving the user data that is communicated to the remote service provider, at least in part,  
14 from the identifying data that identifies the user;  
15 archiving received identifying data in a data storage element of the remote service provider  
16 for each unique identification code; and  
17 comparing the received identifying data for a given unique identification code with  
18 previously archived identifying data for the same unique identification code to determine whether  
19 they match each other.

20  
21 65. (New) The method as in Claim 64 including the step of restricting transmission of said service  
22 data to the user's computer if said received identifying data for a given unique identification code  
23 does not match previously archived identifying data for the same unique identification code.

24  
25 66. (New) A system for preventing piracy of a given software application, said software  
26 application having a unique identification code associated therewith, and said software application  
27 requiring service data to activate at least part of the functionality of said software application, said  
28 system comprising:

1 a user computer system on which a user desires to operate the software application, said user  
2 system being connected to a communications network to transmit user data and to receive said  
3 service data, said user data being derived at least in part from identifying data which identifies the  
4 user, and being derived at least in part from said unique identification code;

5 a remote service computer system connected to said communications network to receive  
6 user data transmitted over the communications network from the user computer system, said remote  
7 service computer system configured to performing the following steps:

8 archiving identifying data received from a user for each unique identification code if no such  
9 identifying data has previously been archived for such unique identification code;

10 comparing received identifying data associated with a unique identification code with  
11 previously archived identifying data corresponding to the same unique identification code if such  
12 identifying data has previously been archived;

13 selectively transmitting service data to the user's computer system over said  
14 communications network when no such identifying data has previously been archived for such  
15 unique identification code;

16 selectively transmitting service data to the user's computer system when it is determined that  
17 the received identifying data is consistent with previously archived data for the same unique  
18 identification code.

19  
20 67. (New) The system as in Claim 66 wherein said service data is maintained by said remote  
21 service computer system in the data storage element used to archive said service data.

22  
23 68. (New) The system as in Claim 66 wherein said service data consists, at least in part, of an  
24 activation code sequence to activate at least part of the functionality of the software application.

25  
26 69. (New) The system as in Claim 66 wherein said service data is transferred by said remote  
27 service computer system without human intervention and received by said user computer system.



1 70. (New) The system as in Claim 66 wherein said remote service computer system manually  
2 transfers said service data from said remote service computer system to said user system.

3  
4 71. (New) The system as in Claim 66 wherein said remote service computer system makes said  
5 service data available to said user from said remote service system, said user being able to  
6 download said service data into said user computer system.

7  
8 72. (New) The system as in Claim 66 wherein said software application includes a program code  
9 sequence that identifies said software application stored on said data storage element of said user  
10 system, said software application additionally being responsive to a second program code sequence  
11 that activates at least part of the functionality of said software application, and which is transmitted  
12 to said user system via a communications network.

13  
14 73. (New) The system as recited in Claim 68 wherein said service data includes at least one  
15 program code sequence that results in a promotional message that may be displayed to said user on  
16 said user computer system.